IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEW MEXICO

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	CRIMINAL NO. 19-3336-MV
	)	
vs.	)	
	)	
FRANCISCO DIAZ,	)	
	)	
Defendant.	)	

UNITED STATES' RESPONSE TO DEFENDANT FRANCISCO DIAZ'S MOTION TO DISMISS THE INDICTMENT FOR GOVERNMENT INFRINGEMENT OF MR. DIAZ'S RIGHT TO COUNSEL

The United States hereby responds to Defendant Francisco Diaz's Motion to Dismiss the Indictment for Government Infringement of Mr. Diaz's Sixth Amendment Right to Counsel (Doc. 166) ("Sixth Amendment Motion"). Defendant's Sixth Amendment Motion lacks merit and should be denied without a hearing.

No member of the trial team has reviewed any attorney-client privileged documents. Pending resolution of this issue, no member of the trial team will review the iCloud data.

To determine whether any such documents even exist within the iCloud data, the United States is in the process of assembling a filter team. That filter team will examine the iCloud data for potentially privileged communications.

If the filter team does not find any privileged communications, and Defendant cannot identify any such communications to the filter team, the Sixth Amendment Motion will be moot.

If the filter team does find privileged communications, any such communications will be withheld from the investigators and prosecutors in this case (collectively the "trial team"). The filter team will provide non-privileged communications and data to defense counsel for review

prior to any disclosure to the trial team. Defense counsel will be afforded an opportunity to submit a privilege log asserting the privilege over any materials from the iCloud account that the filter team has deemed non-privileged.

I. RELEVANT FACTS

A. Events in 2019

On September 3, 2019, officers with the Region III Narcotics Task Force and Drug Enforcement Administration ("DEA") (collectively, "agents") executed a warrant authorizing the search of 7 Josephine Road, Defendant's large walled property in Santa Fe. Agents had obtained that search warrant after a series of four controlled purchases of cocaine from Defendant at this address.

Agents questioned Defendant in his bedroom. He waived his *Miranda* rights and agreed to answer their questions. After agents asked Defendant about drugs in the residence, he directed them to the stash of cocaine in his master bedroom closet. He gave a detailed account of his cocaine sales, dilution methods, and profits. When agents asked Defendant about firearms, he directed them to two pistols within the same closet. Immediately under the pistols, agents located a loaded magazine. The same cabinet contained a box of .40 caliber ammunition, as well as vials of testosterone. As agents interviewed Defendant, he attempted to conceal a checkbook within the master bedroom. That checkbook contained over $10,000 in cash.

Agents arrested Defendant and seized, among other devices, an iPhone in a black case. They identified this device internally as "N-26." Agents placed the iPhone into airplane mode immediately upon seizing it. They then checked it into evidence.

On September 12, 2019, Defendant gave written consent to searches of his devices, including the iPhone. Agents promptly attempted to search these devices. The limits of Cellebrite technology in 2019 prevented them from extracting useful content from the iPhone.

B. Renewed Attempts to Access the iPhone

On April 26, 2023, the United States (through DEA Task Force Officer Thomas Novicki) obtained a search warrant for the iPhone. *See* 23-mr-867. On May 9, 2023, examiners at the Regional Computer Forensics Laboratory ("RCFL") attempted to extract data from the iPhone without success. Agents cancelled the extraction on May 22, 2023, because examiners estimated it would take 24 years to unlock the iPhone.

On August 17, 2023, Defendant's new counsel conveyed to government counsel that Defendant had forgotten his phone password.

On September 28, 2023, a supervisor at RCFL informed agents that the laboratory was willing to make a second attempt to access the iPhone. The supervisor suggested that software updates between May 9, 2023 and September 28, 2023 might make it possible to access the iPhone.

On September 29, 2023, the United States (through DEA Task Force Officer Thomas Novicki) obtained the another search warrant for the iPhone. *See* 23-mr-1868. The resulting attempt, like the first attempt, was unsuccessful.

On October 27, 2023, the United States obtained a third warrant to access the iPhone. This time, the warrant was issued in the District of Columbia and allowed the Computer Crime and Intellectual Property Section's Cybercrime Laboratory to attempt to access the device. The Cybercrime Laboratory was able to create a "Preliminary Device Report" including limited data on the iPhone. The Preliminary Device Report listed the Apple ID as fdiazjr82@me.com, and the associated phone number as 15054903533.

On November 13, 2023, the United States obtained a search warrant, which sought information associated with fdiazjr82@me.com and 15054903533 stored at premises controlled by Apple, Inc. ("Apple").

On November 28, 2023, Apple provided a response to the search warrant in the form of emails with links to files encrypted with GPG software. These links were confusing and nearly impossible to review. The following day, the United States forwarded Apple's email to the Computer Crime and Intellectual Property Section's Cybercrime Laboratory to try to assemble the data in a usable format. The same day (November 29, 2023), the Cybercrime Laboratory provided a zip file containing Cellebrite extractions for the iCloud account.

Assistant U.S. Attorney Hirsch downloaded these files on November 30, 2023, but did not access them for several days. On December 4, 2023, the United States produced the zip file with Cellebrite extractions to defense counsel.

C. Review

Three personnel within the Department of Justice have had access to the iCloud data: Assistant U.S. Attorney Hirsch, the examiner from the Cybercrime Laboratory, and a DEA Intelligence Analyst.

1. Cybercrime Laboratory Examiner

The Cybercrime Laboratory Examiner has no continuing contact with the trial team, and was involved only in creating usable Cellebrite extractions from unusable Apple productions.

2. Assistant U.S. Attorney Hirsch

Assistant U.S. Attorney Hirsch began to review the iCloud data shortly before providing it to defense counsel on December 4, 2023. However, due to the volume of the data and Assistant U.S. Attorney Hirsch's other responsibilities, he only reviewed a small portion of the data.

Assistant U.S. Attorney Hirsch did not view any privileged communications or information of any kind. Indeed, until Defendant brought his Sixth Amendment Motion, the government was unaware that defendant may have communicated with counsel from the Apple account associated with the telephone seized in September 2019. The United States did not intend to encroach upon attorney-client communications, and upon receipt of Defendant's Sixth Amendment Motion immediately suspended review of the iCloud data pending review by a filter team.

3. DEA Intelligence Analyst

Given the volume of the iCloud data and Assistant U.S. Attorney Hirsch's other responsibilities, he did not conduct a review of all of that data. Instead, on the afternoon of December 7, 2023, Assistant U.S. Attorney Hirsch provided a DEA intelligence analyst with a copy of a portion of the iCloud data. He instructed the analyst to review the photos and videos for evidence of drug trafficking or related firearms possession.

Defendant filed the Sixth Amendment Motion at 9:55 p.m. on December 7, 2023.

On December 8, 2023—after receiving the Sixth Amendment Motion—Assistant U.S. Attorney Hirsch instructed the analyst to cease reviewing the production and not to share any results with anyone.

II. RELEVANT LAW

A. General Sixth Amendment Principles

The Sixth Amendment guarantees each criminal defendant the right to effective assistance of counsel. Interference with or intrusion into the attorney-client relationship may violate the Sixth Amendment's guarantee of effective assistance of counsel. *See Weatherford v. Bursey*, 429 U.S. 545, 550 (1977).

B. *Shillinger*

The Tenth Circuit examined severe intrusions into the attorney-client privilege in *Shillinger v. Haworth*. *See* 70 F.3d 1132, 1141 (10th Cir. 1995). There, the court reviewed a District Court's grant of a writ of habeas corpus from a defendant in an Oklahoma state case. That defendant met with his counsel in a courtroom with a deputy sheriff present. *Id.* at 1134. The deputy then reported the substance of the attorney-client conversations to the prosecutor. *Id.* When the defendant testified, the prosecutor cross-examined him using the contents of his conversations with his attorney. *Id.* at 1135. The defendant repeatedly appealed his conviction, giving the Tenth Circuit an opportunity to set out its position on a Circuit split. *See Id.* at 1139-40.

The Tenth Circuit's holding was clear, but limited to situations involving purposeful and unjustified intrusions:

> [W]e hold that when the state becomes privy to confidential communications because of its *purposeful intrusion* into the attorney-client relationship *and lacks a legitimate justification* for doing so, a prejudicial effect on the reliability of the trial process must be presumed.

Id. at 1140 (emphasis added). Even in the extreme situations covered by this holding, the Tenth Circuit explained that the remedy had to be "tailored to the injury suffered from the constitutional violation and should not unnecessarily infringe on competing interests." *Id.* at 1142 (quoting *United States v. Morrison*, 449 U.S. 361, 361–62 (1981)). It mentioned potential remedies including suppression of the evidence obtained through the intrusion and, in cases involving "pervasive[]" taint to the "entire proceeding," retrial by a new prosecutor. *Id.* at 1143. Dismissal of the indictment, it added, could be appropriate in "extreme circumstances," such as when "the government permanently loses potentially exculpatory evidence." *Id.*

C. Non-Purposeful or Justified Intrusions

When intrusions are neither purposeful nor unjustified, or even one of the two factors is present, the outcomes are very different. A showing of prejudice is required. *See Reali v. Abbot*, 90 F. App'x 319, 323 (10th Cir. 2004) (unpublished) ("In the attorney-client privilege context, we presume prejudice only 'when the state becomes privy to confidential communications because of its purposeful intrusion into the attorney-client relationship and lacks a legitimate justification for doing so.'") (quoting *Shillinger*).

In *United States v. Morrison*, DEA agents knowingly circumvented a defendant's counsel to seek her cooperation in a related investigation. 449 U.S. at 362. They disparaged the defendant's counsel, and threatened a stiff jail time if she pressed forward with trial. *Id.* The Third Circuit held that her Sixth Amendment rights "had been violated and that whether or not any tangible effect upon respondent's representation had been demonstrated or alleged, the appropriate remedy was dismissal of the indictment with prejudice." *Id.* at 363. The Supreme Court reversed. *Id.* at 364. It explained that a showing of "demonstrable prejudice, or substantial threat thereof," was required for dismissal. *Id.* at 365. Absent such a showing, there was "no justification for interfering with the criminal proceedings . . . much less the drastic relief granted by the Court of Appeals." *Id.* at 366-67.

In practice, the "Tenth Circuit has almost categorically rejected dismissal of the indictment as a proper remedy in federal prosecutions involving breach of the attorney-client privilege." *United States v. Kaufman*, No. CRIM.A.04-40141-01, 2005 WL 2087759, at *4 (D. Kan. Aug. 25, 2005). There may be no change to the proceedings at all. In *Kaufman*, government agents executing facially valid search warrants seized a large number of documents from the defendant's residence. 2005 WL 2087759, at *4. The defendant argued, without requesting an evidentiary

hearing, that prosecutors "must have read the contents of at least some privileged documents" and demanded dismissal of the indictment. *Id*. The district court rejected their argument:

> with the exception of *Shillinger v. Haworth,* defendants have failed to cite, much less distinguish, the clearly applicable and easily-found Tenth Circuit cases which discuss and reject dismissal of the indictment as an appropriate remedy.[1] This failure has impaired the court's willingness to accept the validity of defendants' factual assertions and other legal arguments.

Id. at *3. The district court also rejected the defendant's demand for a different prosecutor, explaining that the *Shillinger* prosecutor "engaged in extraordinary misconduct for the specific purpose of obtaining privileged information." *Id.* at *5. The court rejected the motion, given that those two "drastic" remedies were the only ones the defendant requested. *Id.* at *6.

III. ANALYSIS

A. The United States did not become privy to confidential communications.

Counsel for the United States has never reviewed any attorney-client privileged communications between Defendant and any of his attorneys. While the declaration of an Assistant U.S. Attorney and officer of this Court should suffice, if the Court believes an *in camera* hearing is necessary, Assistant U.S. Attorney Hirsch will make this averment under oath.

B. There was no purposeful intrusion into the attorney-client relationship.

The United States did not purposefully intrude into Defendant's relationship with his attorneys. Agents did not intentionally circumvent defense counsel by separately approaching Defendant and suggesting that she could not adequately represent his interests. *See Morrison*, 449 U.S. at 362 (refusing to dismiss indictment with prejudice). The United States did not rely on an informant to repeat Defendant's privileged discussions with his client. *See Shillinger v. Haworth*,

[1] *See, e.g.*, *United States v. Singleton*, 52 F. App'x 456, 459 (10th Cir. 2002).

70 F.3d at 1141 (remanding for development of record). Agents did not purposefully make copies of a document defendant claimed contained copies of his discussions with his counsel. *See United States v. Lin Lyn Trading, Ltd.*, 149 F.3d 1112, 1117 (10th Cir. 1998) (refusing to dismiss indictment with prejudice). Instead, the United States obtained a facially valid search warrant for the contents of an iCloud account in order to search for evidence of violations of 21 U.S.C. §§ 841(a)(1) and 846, as well as 18 U.S.C. § 924(c). Government counsel timely produced a copy of that data for Defendant. No one on the prosecution team had any knowledge that Defendant allegedly used messages or emails backed up to that account to communicate with his counsel.

C. The United States had a legitimate justification to seek the iCloud data: its interest in effective law enforcement.

The United States did not deliberately intrude into an attorney-client relationship "to learn what it could about the defendant's defense plans[.]" *Weatherford*, 429 U.S. at 557. Given the encryption technology available to even unsophisticated criminals through Apple, Facebook, and other means, search warrants for the devices seized at the time of arrest will not always bear fruit. The existence of electronic backup systems provides a necessary tool to circumvent this encryption. Defendant might prefer that the United States' investigation into his (and his supplier's) crimes end immediately upon his indictment, but there is no legal basis for that preference.

D. Even assuming arguendo that an intentional intrusion occurred without any legitimate justification, the proper remedy would then be suppression.

Supreme Court precedent bars dismissal with prejudice here. In *United States v. Morrison*, the Court explained that "Cases involving Sixth Amendment deprivations are subject to the general rule that remedies should be tailored to the injury suffered from the constitutional violation and should not unnecessarily infringe on competing interests." 449 U.S. at 364. These interests

include "society's interest in the administration of criminal justice." *Id.* Accordingly, courts must "identify and then neutralize the taint by tailoring relief appropriate in the circumstances to assure the defendant the effective assistance of counsel and a fair trial." *Id.*

None of Defendant's cited cases, including *Shillinger*, countenanced dismissal with prejudice where other remedies were available. A failure to consider alternative remedies to the dismissal of an indictment is an abuse of discretion. *See Lin Lyn Trading, Ltd.*, 149 F.3d at 1118.

E. The United States' proposed procedure more than adequately addresses Defendant's claims about the attorney-client privilege.

No member of the trial team has reviewed, or will review, any attorney-client privileged materials. If such materials exist in the iCloud data, the filter team will screen them out, and Defendant will review any resulting files before they are produced to the trial team. The government has also requested defense counsel's assistance in this endeavor to accurately identify any and all communications to or from the defense team's telephone numbers, email addresses, and social media accounts. This procedure will protect Defendant's Sixth Amendment rights while vindicating the public's interest in effective law enforcement.[2] *See Eastman v. United States*, 615 F. Supp. 3d 1250, 1258 (D.N.M. 2022) (describing use of filter teams); *In re Sealed Search Warrant & Application for a Warrant by Tel. or Other Reliable Elec. Means*, No. 20-03278-MJ, 2020 WL 6689045, at *2 (S.D. Fla. Nov. 2, 2020), *aff'd*, 11 F.4th 1235 (11th Cir. 2021).

[2] Although the United States concedes that the use of a filter team would have been preferable from the start, it had no knowledge that Defendant's privileged communications even potentially could appear in the iCloud data.

IV. CONCLUSION

For the foregoing reasons, the United States respectfully requests that the Court deny Defendant's Sixth Amendment Motion and permit counsel to bring this case to a close.

Respectfully submitted,

ALEXANDER M.M. UBALLEZ
United States Attorney

/s/ Electronically filed on 12/11/2023
David B. Hirsch
Assistant United States Attorney
P.O. Box 607
Albuquerque, New Mexico 87103
(505) 346-7274

I HEREBY CERTIFY that on December 11, 2023,
I filed the foregoing pleading
electronically through the CM/ECF system,
which caused counsel of record to be served
by electronic means.

/s/ Electronically filed on 12/11/23
David B. Hirsch
Assistant United States Attorney